

[First Hit](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

Generate Collection

Print

L2: Entry 15 of 74

File: JPAB

Oct 13, 1995

PUB-NO: JP407262455A

DOCUMENT-IDENTIFIER: JP 07262455 A

TITLE: TRANSACTION PROCESSING SYSTEM

PUBN-DATE: October 13, 1995

## INVENTOR-INFORMATION:

NAME

COUNTRY

NAKATSUJI, KUNITOSHI

## ASSIGNEE-INFORMATION:

NAME

COUNTRY

OMRON CORP

APPL-NO: JP06048942

APPL-DATE: March 18, 1994

INT-CL (IPC): G07G 1/12

## ABSTRACT:

PURPOSE: To provide a transaction processing system capable of reducing the frequency of generating bad bonds and efficiently executing transaction processing by determining an authentication processing method based on a transaction amount and a transaction amount paying method.

CONSTITUTION: A terminal equipment 1 transmits authentication data including card data such as a card number read out from a card held by a customer and transaction data including an inputted transaction amount and a transaction amount paying method to a host device 2 through a data transmission line. At the time of receiving the authentication data from the equipment 1, the device 2 judges whether the authentication of the transaction is to be executed by simple authentication processing or master authentication processing based upon a limited amount file 8 and the authentication data. When the transaction authentication is judged to be executed by using simple authentication processing, the device 2 executes the authentication of the transaction by using a negative file 7b, and when the transaction authentication is judged to be executed by using the master authentication processing, the device 2 transmits authentication data to a master device 4. At the time of receiving the authentication data from the device 2, the device 4 executes transaction authentication processing by using a customer information file 6 and a negative file 7a.

COPYRIGHT: (C)1995,JPO

[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-262455

(43) 公開日 平成7年(1995)10月13日

(51) Int.Cl.<sup>°</sup>

G 0 7 G 1/12

識別記号

3 2 1 P

庁内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数4 O L (全 7 頁)

(21) 出願番号 特願平6-48942

(22) 出願日 平成6年(1994)3月18日

(71) 出願人 000002945

オムロン株式会社

京都府京都市右京区花園土堂町10番地

(72) 発明者 中辻 都登志

京都府京都市右京区花園土堂町10番地 オムロン株式会社内

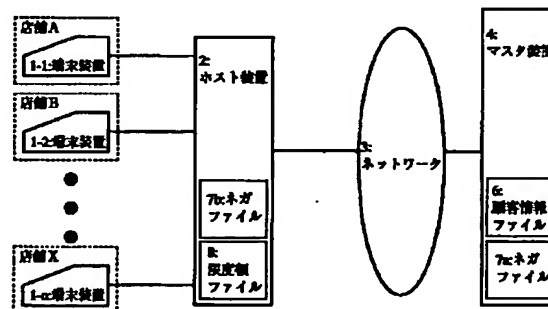
(74) 代理人 弁理士 小森 久夫

(54) 【発明の名称】 取引処理システム

(57) 【要約】

【目的】取引金額と取引金額の支払い方法によって認証処理の方法を決定することにより、不良債券の発生を低下させるとともに取引処理を効率的に処理することができる取引処理システムを提供する。

【構成】端末装置1は、顧客が所有するカードから読みだしたカード番号等のカードデータと入力された取引金額や取引金額の支払い方法を含む取引データとを含む認証用データをデータ伝送ラインを介してホスト装置2に送信する。ホスト装置2は端末装置1から認証用データを受信すると、限度額ファイル8と認証用データから取引の認証を簡易認証処理で行うか、マスタ認証処理で行うかを判定する。ホスト装置2は、取引の認証を簡易認証処理で行うと判定するとネガファイル7bを用いて取引の認証を行い、取引の認証をマスタ認証処理で行うと判定するとマスタ装置4に認証用データを送信する。マスタ装置4は、ホスト装置から認証用データが送信されてくると顧客情報ファイル6とネガファイル7aを用いて取引の認証処理を行う。



## 【特許請求の範囲】

【請求項1】 顧客が所有するカードからカード番号等のカードデータを読み出すカードデータ読出手段と、取引金額や取引金額の支払い方法を含む取引データを入力する取引データ入力手段と、前記カードデータと取引データを含む認証用データを出力する認証用データ出力手段と、を備えた端末装置と、

前記端末装置が複数接続され、無効となったカードに与えられていたカード番号を登録したネガファイルを記憶するネガファイル記憶手段と、カード毎に所有する顧客の与信限度額や現在の債務額等の顧客情報を記憶する顧客情報記憶手段と、前記ネガファイルのみを用いて取引の認証を行う簡易認証処理手段と、前記ネガファイルと顧客情報を用いて取引の認証を行う正規の認証処理手段と、簡易認証処理で認証する取引を制限する認証方法制限手段と、を備えた認証処理装置と、を備え、前記認証方法制限手段は、簡易認証処理で取引を認証するかどうかを取引金額の支払い方法で制限する手段であることを特徴とする取引処理システム。

【請求項2】 支払い方法に対応させて取引の認証が簡易認証処理で行える取引金額の限度額を設定した限度額ファイルを記憶する限度額ファイル記憶手段を備え、前記認証方法制限手段は、取引金額の支払い方法とともに前記限度額を用いて簡易認証処理で取引を認証するかどうかを制限し、取引金額が該当する支払い方法の限度額未満の時に取引の認証を簡易認証処理で行うと判定する手段を含むことを特徴とする請求項1記載の取引処理システム。

【請求項3】 前記端末装置は、複数の店舗に設置され、前記限度額ファイルは、店舗毎に取引金額の支払い方法に対応させて限度額を登録したファイルであることを特徴とする請求項2記載の取引処理システム。

【請求項4】 前記限度額ファイルは、商品毎に取引金額の支払い方法に対応させて限度額を登録したファイルであることを特徴とする請求項2記載の取引処理システム。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】この発明は、クレジットカードを使用して取引処理を行う取引処理システムに関し、特に取引金額と取引金額の支払い方法に基づいて取引の認証方法を決定する取引処理システムに関する。

## 【0002】

【従来の技術】クレジットカードを使用して取引処理を行う取引処理システムは、入力操作を行うC A T等の端末装置にデータ伝送ラインを介してホスト装置が接続され、前記ホスト装置にはネットワークを介してクレジットカード会社のマスタ装置が接続されている。従来の取引処理システムでは、端末装置は認証用データ（カード

に記憶されているカードデータや取引内容を示す取引データ）がオペレータによって入力されると、この認証用データをホスト装置、ネットワークを介してカード会社のマスタ装置に送信する。この認証用データを受信したマスタ装置は、自分が記憶している認証用ファイルを利用し、この認証用ファイルに基づいてカードの有効、無効や与信限度額のチェック等を行って、取引の可否を判定し、認証結果をネットワーク、ホスト装置を介して端末装置に送信する。

10 【0003】この様に、取引の認証処理をクレジットカード会社のマスタ装置で行うマスタ認証処理方式がある（図7参照）。

【0004】一方、取引毎に取引の認証をマスタ認証処理方式で行うとマスタ装置の負荷が増大するとともに、マスタ装置に接続される回線のトラフィック量が大きくなりすぎて取引の認証処理が非効率的となる場合がある。そこで、無効となったカードに与えられていたカード番号を登録したネガファイルをホスト装置に記憶し、ホスト装置にてこのファイルを利用してカードの有効、無効のみを判定することで取引の認証を行う簡易認証処理方式が採用されることがある（図8参照）。この方式では、定期的にホスト装置に記憶されている取引データをカード会社のマスタ装置側に上げるバッチ処理が必要となる。この簡易認証処理方式を採用すると、取引の認証を効率的に行うことができるが、取引の認証時に顧客の与信限度額がチェックされず不良債券が発生する問題がある。

20 【0005】そこで、従来の取引処理システムは取引の処理を効率的に行うためにホスト装置に取引金額の限度額（この取引金額ではカードに与えられている与信限度額を越えないと思われる金額）を設定し、この限度額以上の場合には上記したマスタ認証処理を行い、限度額未満の場合には簡易認証処理を行うようにしていた。

## 【0006】

30 【発明が解決しようとする課題】しかしながら、簡易認証処理方式では与信限度額のチェックが行われないので、繰り返し限度額未満の取引を行うと、債務額が与信限度額を越えてしまう。特に、取引金額を分割払いやリボルビング払い等の場合には、以前に取引した取引金額の支払いが完了していない顧客は債務が残っており、限度額未満の取引でもすぐに債務額が与信限度額以上になってしまうため、不良債券が発生する頻度が高かった。

40 【0007】ここで、全ての取引の認証をカード会社のマスタ装置で行うマスタ認証処理方式を採用することも考えられるが、上記したように特にクレジットカードを使用した取引が多い百貨店や大型店舗では、認証処理に要する時間が長くなり取引処理が非効率的になってしまう。

50 【0008】この発明の目的は、取引金額と取引金額の支払い方法によって認証処理の方法を決定することによ

り、不良債券の発生を低下させるとともに取引処理を効率的に処理することができ取引処理システムを提供することにある。

【0009】

【課題を解決するための手段】この発明の取引処理システムは、顧客が所有するカードからカード番号等のカードデータを読み出すカードデータ読出手段と、取引金額や取引金額の支払い方法を含む取引データを入力する取引データ入力手段と、前記カードデータと取引データを含む認証用データを出力する認証用データ出力手段と、を備えた端末装置と、前記端末装置が複数接続され、無効となったカードに与えられていたカード番号を登録したネガファイル記憶するネガファイル記憶手段と、カード毎に所有する顧客の与信限度額や現在の債務額等の顧客情報を記憶する顧客情報記憶手段と、前記ネガファイルのみを用いて取引の認証を行う簡易認証処理手段と、前記ネガファイルと顧客情報を用いて取引の認証を行う正規の認証処理手段と、簡易認証処理で認証する取引を制限する認証方法制限手段と、を備えた認証処理装置と、を備え、前記認証方法制限手段は、簡易認証処理で取引を認証するかどうかを取引金額の支払い方法で制限する手段であることを特徴とする。

【0010】また、支払い方法に対応させて取引の認証が簡易認証処理で行える取引金額の限度額を設定した限度額ファイルを記憶する限度額ファイル記憶手段を備え、前記認証方法制限手段は、取引金額の支払い方法とともに前記限度額を用いて簡易認証処理で取引を認証するかどうかを制限し、取引金額が該当する支払い方法の限度額未満の時に取引の認証を簡易認証処理で行うと判定する手段を含むことを特徴とする。

【0011】また、前記端末装置は、複数の店舗に設置され、前記限度額ファイルは、店舗毎に取引金額の支払い方法に対応させて限度額を登録したファイルであることを特徴とする。

【0012】また、前記限度額ファイルは、商品毎に取引金額の支払い方法に対応させて限度額を登録したファイルであることを特徴とする。

【0013】

【作用】この発明の取引処理システムにおいては、端末装置が入力された取引金額や取引金額の支払い方法を含む取引データと、カードから読み出したカードデータを認証用データとして出力する。認証処理装置は、端末装置が出力した認証用データを読み込むと、認証用データに含まれる取引金額の支払い方法を読み出す。そして、この取引金額の支払い方法で認証処理を簡易認証処理または正規の認証処理のどちらで実行するかを判定する。したがって、簡易認証処理または正規の認証処理のどちらで取引の認証を行うかを取引金額の支払い方法で設定することができる。

【0014】また、認証処理装置は、限度額ファイルに

登録されている該当する支払い方法の限度額と取引金額を用いて取引の認証処理を簡易認証処理または正規の認証処理のどちらで実行するかを判定する。したがって、簡易認証処理または正規の認証処理のどちらで取引の認証を行うかを取引金額と取引金額の支払い方法で設定することができる。

【0015】また、店舗毎に取引金額の支払い方法に対応させて限度額を登録することにより、各店舗で取引の認証処理を簡易認証処理または認証処理のどちらで行うかを設定することができる。

【0016】また、商品毎に取引金額の支払い方法に対応させて限度額を登録することにより、各商品で取引の認証処理を簡易認証処理または認証処理のどちらで行うかを設定することができる。

【0017】

【実施例】図1は、この発明の実施例である取引処理システムの構成を示す図である。取引処理システムは、店舗に設置されたクレジットカードを使用した取引等を処理する端末装置1(1-1~1-n)と、複数の前記端末装置1とデータ伝送ラインで接続されたホスト装置2と、前記ホスト装置2と公衆回線網等のネットワーク3を介して接続されたカード会社のマスタ装置4と、を備えている。端末装置1は、複数の店舗に設置されている。カード会社のマスタ装置4には、発行されているクレジットカード毎にカード番号に対応させて顧客の氏名、住所、与信限度額、現在の債務額等の顧客情報が記憶された顧客レコードを登録した顧客情報ファイル6と、無効となったカードに与えられていたカード番号が登録されているネガファイル7aとを備えている。ホスト装置2には、無効となったカードに与えられていたカード番号が登録されているネガファイル7bと、簡易認証処理(ホスト装置でのネガチェックのみで取引の可否を判定する取引の認証方法)で認証する取引を制限するデータとして取引金額の支払い方法(債務額を一括して支払う一括払い、債務額に関係なく一定の金額ずつ支払うリボルビング払い、取引金額を分割回数で分割して支払う分割払い等)に取引の認証を簡易認証処理で行うと判定する限度額を対応させて登録した限度額ファイル8とを備えている。前記ホスト装置2とネットワーク3を介して接続されたカード会社のマスタ装置4とでこの発明の認証処理装置を構成する。

【0018】取引の認証には、ホスト装置2でネガファイル7bを用いて取引の可否を判定する簡易認証処理方式と、マスタ装置4でネガファイル7aと顧客情報ファイル6を用いて取引の可否を判定するマスタ認証処理方式(正規の認証処理)との2つの方法がある。

【0019】図2は、ホスト装置2の構成を示すブロック図である。ホスト装置2は、CPU11と、ROM12と、RAM13と、無効となったクレジットカードに与えられていたカード番号が登録されているネガファイ

ル7bを記憶するネガファイル記憶部14と、前記限度額ファイル8を記憶する限度額ファイル記憶部15と、端末装置1とデータ通信を行う下位通信部16と、カード会社のマスタ装置4とネットワーク3を介してデータ通信を行う上位通信部17とを備えている。限度額ファイル8には、店舗を識別する店舗コードを記憶する店舗コード記憶エリア21と、取引金額の支払い方法が一括払いの際の限度額を記憶する一括払い限度額記憶エリア22と、取引金額の支払い方法が分割払いの際の限度額を記憶する分割払い限度額記憶エリア23と、取引金額の支払い方法がリボルビング払いの際の限度額を記憶するリボルビング払い限度額記憶エリア24と、を備えた限度額レコード25がホスト装置2に接続されている端末装置1を設置している店舗毎に登録されている(図3参照)。

【0020】図4は、端末装置の構成を示すブロック図である。端末装置1は、CPU31と、ROM32と、RAM33と、顧客が所有するクレジットカードからカードデータを読み出すカード処理部34と、取引金額や取引金額の支払い方法等の取引データを入力する入力部35と、取引の認証結果等を表示する表示部36と、取引伝票を印字して発行するプリント部37と、データ伝送ラインで接続されているホスト装置2とデータ通信を行う通信部38とを備えている。

【0021】図5は、同取引処理システムでのクレジットカードを使用した取引の認証処理の流れを示す図である。店舗でクレジットカードを使用した取引を行う場合、オペレータが端末装置1のカード処理部34に顧客が所有するクレジットカードを挿入する。端末装置1はカード処理部34に挿入されたクレジットカードからカード番号等のカードデータを読み出し、このカードデータをRAM33に一旦記憶する(n1)。そして、端末装置1は入力部35から取引する商品を識別する商品コード、取引金額、取引金額の支払い方法等が取引データの入力を受け付ける(n2)。オペレータは、入力部35を操作して取引データの入力を行う。端末装置1は、取引データが入力されると、n1で読みだしたカードデータと取引データを含む認証用データを作成し(n3)、この作成した認証用データを通信部38からデータ伝送ラインに出力する(n4)。

【0022】ホスト装置2は、端末装置1がn4でデータ伝送ラインに出力した認証用データを下位通信部17で受信すると(n11)、この認証用データに含まれる取引金額と取引金額の支払い方法を読み出す(n12)。そして、限度額ファイル8から該当する店舗の限度額レコード25を検索し(n13)、該当する支払い方法に対応して記憶している限度額と取引金額を比較する(n14)。n14の比較で取引金額が限度額未満の場合にはこの取引の認証を簡易認証処理で行うと判定し、取引金額が限度額以上の場合にはこの取引の認証を

マスタ認証処理で行うと判定する。例えば、該当する店舗の顧客レコード25に、

一括払い 限度額30000

分割払い 限度額15000円

リボルビング払い 限度額15000円と登録されていると(図3の店舗Aの場合)、取引金額が20000円の場合、取引金額の支払い方法が一括払いであれば取引の認証を簡易認証処理で行い、取引金額の支払い方法がリボルビング払いまたは分割払いであると取引の認証をマスタ認証処理で行うと判定する。

【0023】ホスト装置2は、取引の認証を簡易認証処理で行うと判定すると、ネガファイル7bに認証用データに含まれるカード番号が登録されているかどうかを判定するネガチェックを行い(n15)、該当するカード番号が登録されていれば取引不可と判定し、該当するカード番号が登録されていなければ取引可と判定する。

【0024】一方、ホスト装置2は、取引の認証をマスタ認証処理で行うと判定すると、カード会社のマスタ装置4に上位通信部17からネットワーク3を介してn11で受信した認証用データを送信する(n16)。

【0025】マスタ装置4は、認証用データを受信すると(n21)、顧客情報ファイル6とネガファイル7aを用いてカードの有効無効や顧客の債務額が与信限度額の範囲内であるかを判定するマスタ認証処理を行い(n22)、取引の可否を判定する。マスタ装置4は取引の可否を判定すると、ホスト装置2に向けてこの認証結果をネットワーク3に出力する。

【0026】ホスト装置2は、マスタ装置4から送信されてきた認証結果を上位通信部17で受信することによりマスタ認証処理が行われた取引の認証結果を獲得する(n17)。そして、ホスト装置2は、取引の認証用データを送信してきた端末装置1に向けて取引の認証結果を下位通信部16からデータ伝送ラインに出力する(n18)。

【0027】端末装置1は、ホスト装置2がn18で出力した認証結果を通信部38で受信すると(n5)、認証結果を表示部36に表示したり、プリント部37で印字する等するの出力処理を行い(n6)、認証結果をオペレータに知らせる。オペレータは、n6で出力処理された認証結果に基づいて顧客との取引処理を行う。

【0028】なお、取引の認証処理を簡易認証処理で行った場合には、ホスト装置2は取引データを一旦RAM13に記憶しておき、後でカード会社のマスタ装置4に取引データを送信するバッチ処理を行う。

【0029】以上のように、取引の認証を簡易認証処理またはマスタ認証処理のどちらで行うかを、取引金額と取引金額の支払い方法に応じて設定することができる。例えば、一括払いに比べて分割払いやリボルビング払いの限度額を低く設定しておくことにより、不良債券の発生する頻度が高い分割払いやリボルビング払いの取引の

認証だけを強化することができる。したがって、不良債券の発生を低下させるとともに取引の認証を効率的に行うことができる。

【0030】また、取引金額の支払い方法に対応させて取引の認証を簡易認証処理で行うかどうかを制限する限度額を店舗毎に登録することができるので、各店舗が自店舗に応じた限度額を設定することができる。

【0031】また、取引金額の支払い方法のみによって取引の認証を簡易認証処理またはマスタ認証処理のどちらで行うかを制限することもできる。この場合には、限度額ファイル8のかわりに、取引金額の支払い方法に対応させて取引の認証を簡易認証処理またはマスタ認証処理のどちらで行うかを登録しておく。ホスト装置2は端

末装置1から送信されてきた認証用データに含まれる取引金額の支払い方法に対応して登録されている認証方法で取引の認証を行う。したがって、簡単に取引の認証を強化することができる。

【0032】また、限度額ファイル8の構成を図6に示すように、商品を識別する商品コードを記憶する商品コード記憶エリア41と、取引金額の支払い方法が一括払いの際の限度額を記憶する一括払い限度額記憶エリア42と、取引金額の支払い方法が分割払いの際の限度額を記憶する分割払い限度額記憶エリア43と、取引金額の支払い方法がリボルビング払いの際の限度額を記憶するリボルビング払い限度額記憶エリア44と、を備えた限度額記録45がホスト装置2に接続されている端末装置1を設置している店舗で販売されている商品毎に登録してもよい。

【0033】この場合には、ホスト装置2は取引の認証を簡易認証処理またはマスタ認証処理のどちらで行うかを判定する場合には、該当する商品の限度額記録45を用いて判定することになる。

【0034】なお、限度額ファイル8に限度額記録45を商品毎に登録する場合には、取引金額の支払い方法に対応させて限度額を登録せずに、取引の認証を簡易認証処理またはマスタ認証処理のどちらで行うかを示すフラグを登録するようにしてもよい。

【0035】

【発明の効果】以上のように、取引の認証を簡易認証処

理またはマスタ認証処理のどちらで行うかを、取引金額の支払い方法で設定することができる。したがって、不良債券の発生する頻度が高い分割払いやリボルビング払いの取引の認証を必ずマスタ認証処理で行わせることができる。すなわち、簡単に取引の認証を強化することができるとともに、効率良く取引を認証することができる。

【0036】また、取引基金額の支払い方法と取引金額に応じて設定することもできるので、例えば、一括払いに比べて分割払いやリボルビング払いの限度額を低く設定しておくことにより、不良債券の発生する頻度が高い分割払いやリボルビング払いの取引の認証だけを強化するとともに、さらに効率よく取引の認証を行うことができる。よって、不良債券の発生を低下させることができる。また、取引の認証を効率的に行うことができる。

【0037】また、取引金額の支払い方法に対応させて取引の認証を簡易認証処理で行うかどうかを制限する限度額を店舗毎や商品毎に登録することができるので、各店舗が自店舗に応じた取引の認証を行うことができる。

【図面の簡単な説明】

【図1】この発明の実施例である取引処理システムの構成を示す図である。

【図2】同実施例のホスト装置の構成を示す図である。

【図3】同取引処理システムの限度額ファイルの構成を示す図である。

【図4】同実施例の端末装置の構成を示す図である。

【図5】同取引処理システムの取引の認証を行う処理の流れを示すフローチャートである。

【図6】この発明の他の実施例における限度額記憶ファイルの構成を示す図である。

【図7】マスタ認証処理の流れを示す図である。

【図8】簡易認証処理の流れを示す図である。

【符号の説明】

1 (1-1~1-n) - 端末装置

2 - ホスト装置

3 - ネットワーク

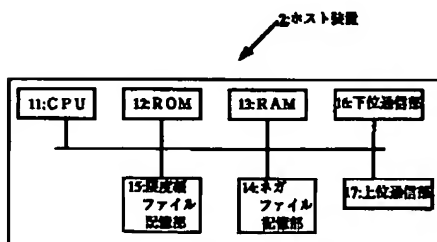
4 - マスタ装置

6 - 顧客情報ファイル

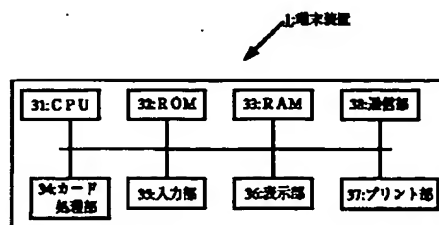
7a、7b - ネガファイル

8 - 限度額ファイル

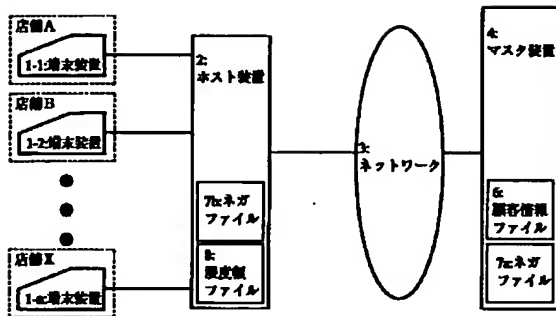
【図2】



【図4】



【図1】



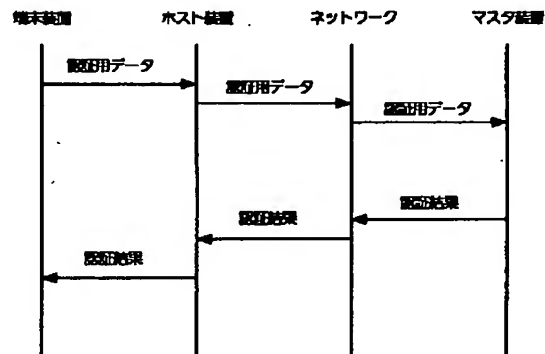
【図3】

店舗名	店舗コード 記号エリア	一括払い振込額 記号エリア	分割払い振込額 記号エリア	リボルディング払い 振込額記号エリア
店舗A	1234	30000	15000	15000
店舗B	1235	50000	25000	20000
店舗C	1236	40000	20000	20000
店舗D	1237	30000	20000	10000

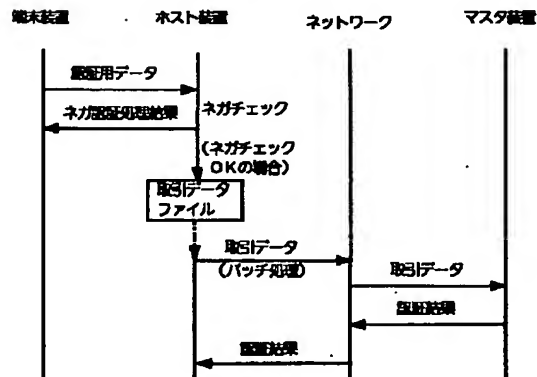
【図6】

商品コード 記号エリア	一括払い振込額 記号エリア	分割払い振込額 記号エリア	リボルディング払い 振込額記号エリア
1234567890	30000	15000	15000
1234567891	50000	25000	20000
1234567892	40000	20000	20000
1234567893	30000	20000	10000

【図7】



【図8】



【図5】

